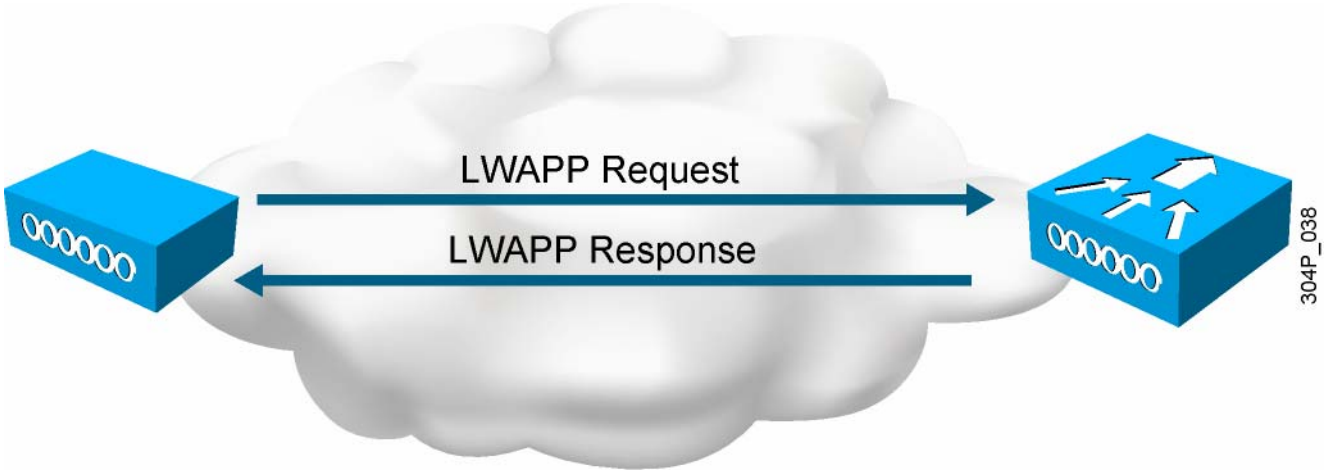
Understanding Wireless Network Controller Technology

Identifying Wireless Networking Considerations

LWAPP Discovery



1. The access point issues a DHCPDISCOVER to get an IP address.
2. If the access point supports Layer 2 LWAPP, attempt Layer 2 discovery.
3. Else, attempt Layer 3 LWAPP discovery.
4. If no WLC response, then access point reboots and returns to Step 1.

Layer 3 LWAPP Discovery Algorithm

- Access point sends Layer 3 LWAPP discovery requests:
  1. As broadcasts on local subnet
  2. As unicast LWAPP discovery requests to WLC IP addresses advertised by other access points, if OTAP enabled on the WLCs
  3. To all previously stored WLC IP addresses
  4. To IP addresses learned through DHCP Option 43
  5. To IP addresses learned through DNS resolution of CISCO-LWAPP-CONTROLLER.localdomain
- WLCs receiving the discovery message reply with a unicast LWAPP discovery response message.
- Access point compiles a list of candidate controllers.

WLC Selection Algorithm

- LWAPP discovery and selection mechanism is a design decision.
- LWAPP discovery response contains WLC information.
- After the LWAPP discovery interval timer, the access point selects a WLC to send an LWAPP join request based on:
  1. Previously configured primary, secondary, or tertiary WLCs (specified in the controller sysName)
  2. WLC configured as a master controller
  3. WLC with the greatest capacity for access point associations
- The WLC validates the access point and sends an LWAPP join response. An encryption key is derived, and future messages are encrypted.

Access Point Operations

- Access point downloads firmware from the WLC if its code version does not match the WLC.
- WLC provisions access point with the SSID, security, QoS, and other parameters.
- WLC periodically queries access points for status.
- Access point periodically sends an LWAPP heartbeat (every 30 seconds):
  - If heartbeat is not acknowledged, the access point resends.
  - If heartbeat is not acknowledged in five attempts, access point looks for a new WLC.

WLC Deployment Considerations

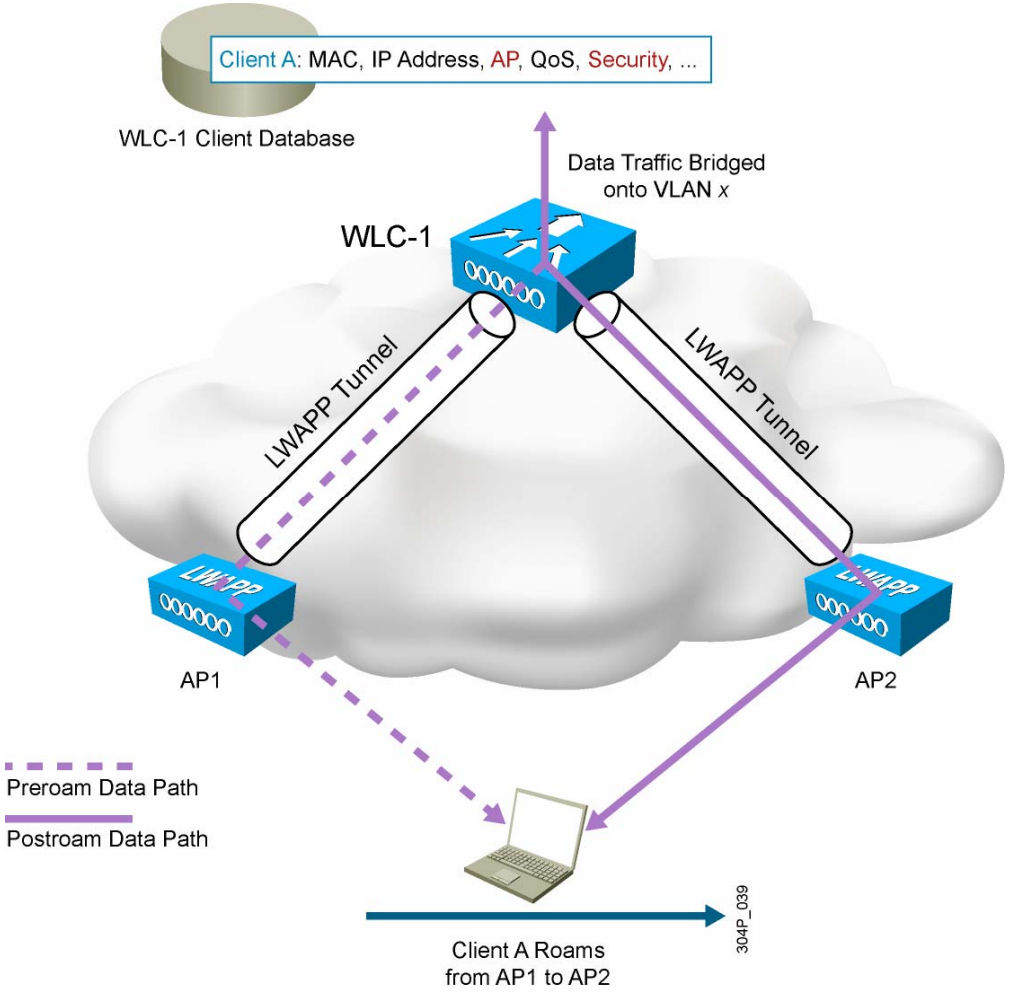
- Mobility
- Radio management
- Redundancy and load balancing
- Scaling
- IP addressing

Mobility Defined

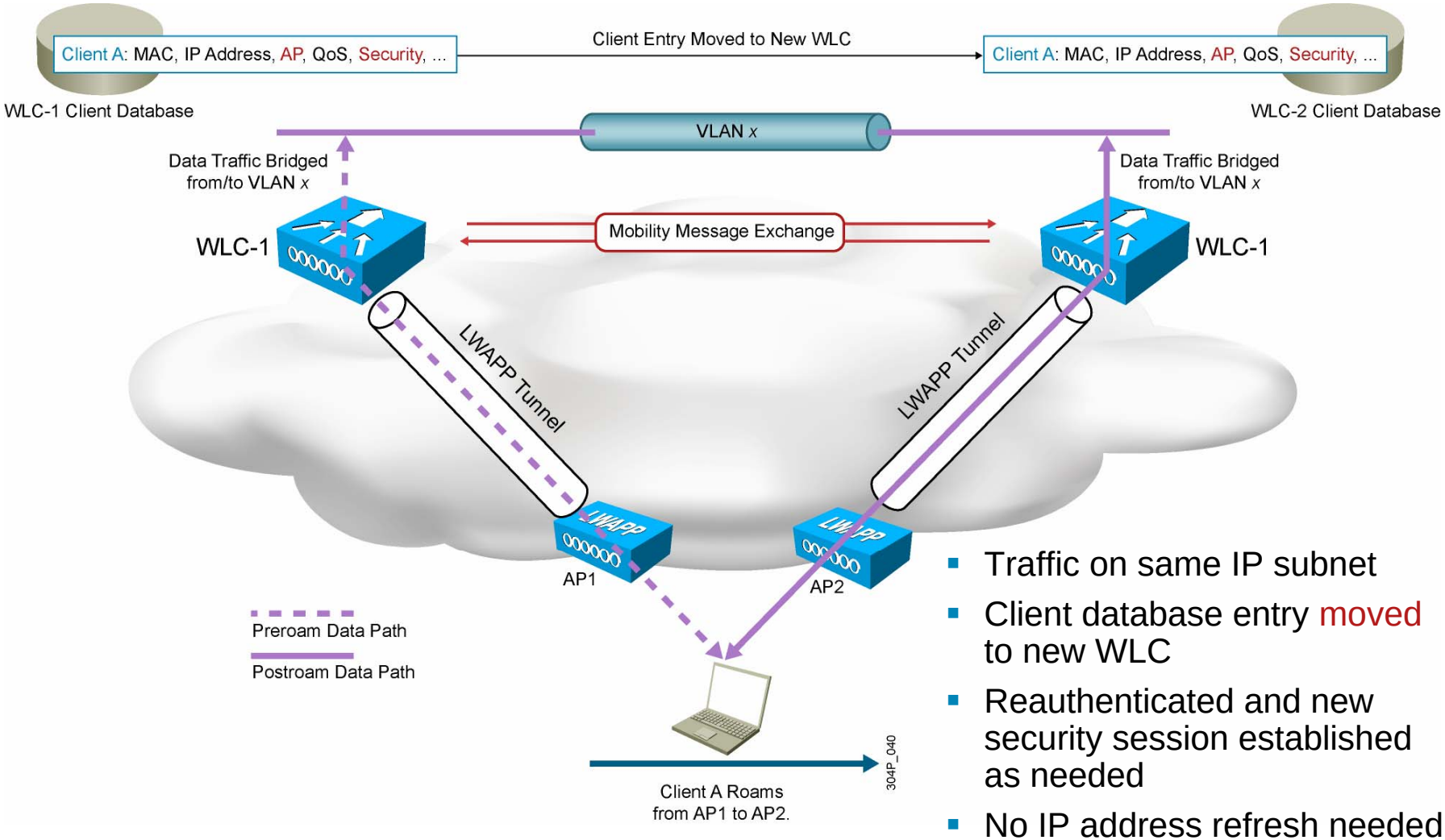
- Mobility is a key reason for wireless networks.
- Mobility means the end-user device is capable of moving to new location.
- Roaming occurs when a wireless client moves association from one access point and reassociates to another.
- Mobility presents new challenges:
  - Need to scale the architecture to support client roaming—roaming can occur intracontroller and intercontroller.
  - Depending on the application, may need to support Layer 2 or Layer 3 roaming.
  - Need to support client roaming that is seamless (fast) and preserves security.

Intracontroller Roaming

- Intracontroller roaming occurs when a client moves association to another access point joined to the same WLC.
- Client may need to be reauthenticated and new security session established.
- Controller updates client database entry with new access point and appropriate security context.
- No IP address refresh is needed.

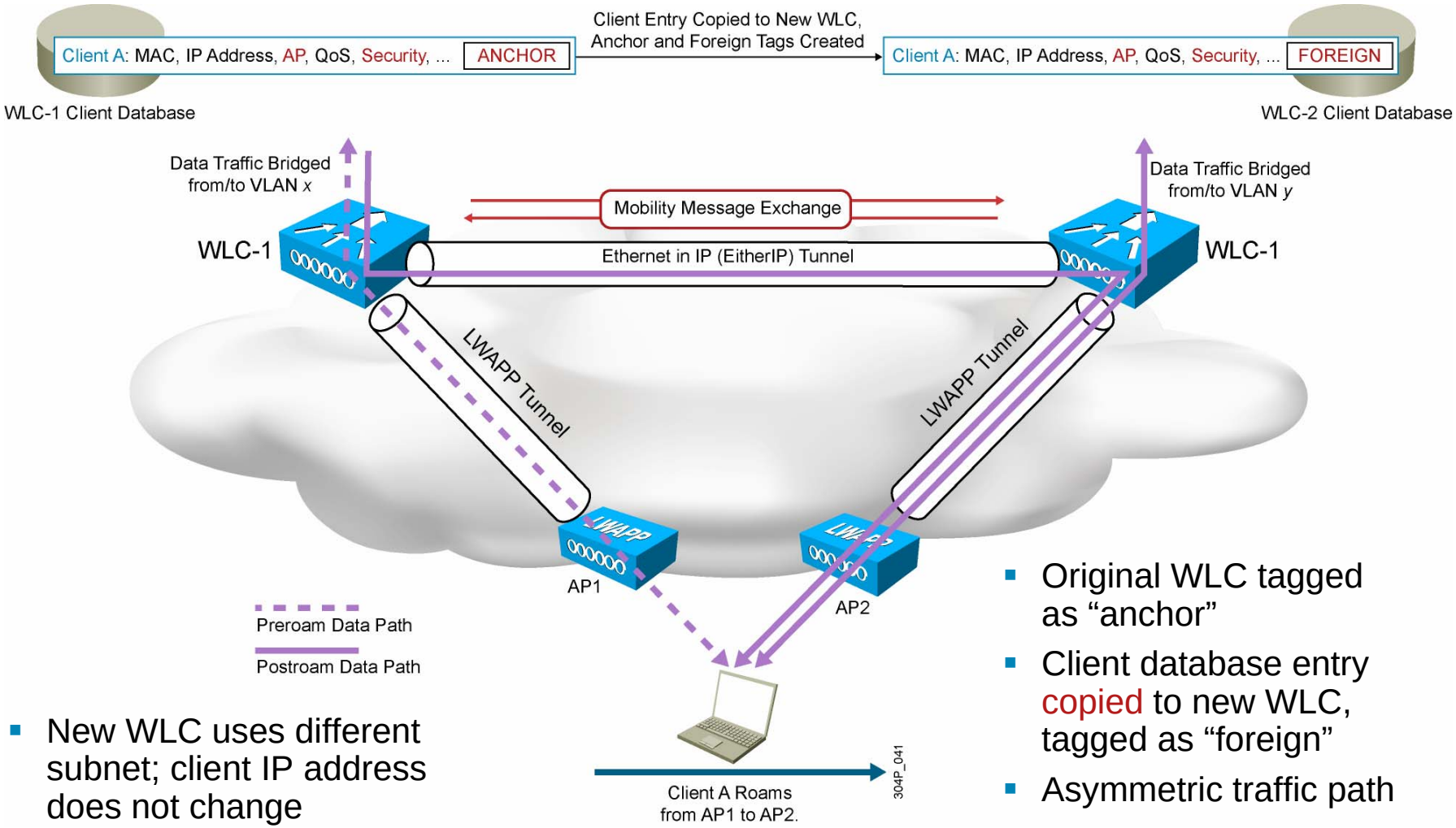


Intercontroller Roaming—Layer 2



- Traffic on same IP subnet
- Client database entry moved to new WLC
- Reauthenticated and new security session established as needed
- No IP address refresh needed

Intercontroller Roaming—Layer 3



- New WLC uses different subnet; client IP address does not change

- Original WLC tagged as “anchor”
- Client database entry copied to new WLC, tagged as “foreign”
- Asymmetric traffic path

Scaling the Architecture with Mobility Groups

- Mobility groups allow controllers to peer with each other to support seamless roaming across controller boundaries, access point load balancing, and controller redundancy.
  - Mobility messages are exchanged between controllers.
  - Data is tunneled between controllers in Ethernet-in-IP (EtherIP).
- Each WLC in a mobility group is configured with a list of other members.
- Access points learn the IP addresses of the other members of the mobility group after the LWAPP join process.
- Mobility groups support up to 24 controllers and 3600 access points.
- WLC should be placed in mobility groups when intercontroller roaming is possible and for controller redundancy.

Mobility Group Requirements

- IP connectivity must exist between the management interfaces of all WLC devices.
- All WLCs must be configured with the same mobility group name. The mobility group name is case-sensitive.
- All WLCs must be configured to use the same virtual interface IP address.
- Each WLC is configured with the MAC address and IP address of all the other mobility group members.
- The WLCs exchange messages using UDP port 16666 (unencrypted) or UDP port 16667 (encrypted) .

Supporting Roaming—Recommended Practices

- Minimize intercontroller roaming in your designs.
- Design the network for <= 10 ms RTT latency between controllers.
- Intercontroller Layer 2 roaming is more efficient than Layer 3 roaming.
- Use PKC or CCKM to speed up and secure roaming.
- Client roaming capabilities vary by vendor, driver, and supplicant. Look for Cisco Compatible Extensions v4 feature set.

Controller Redundancy Design

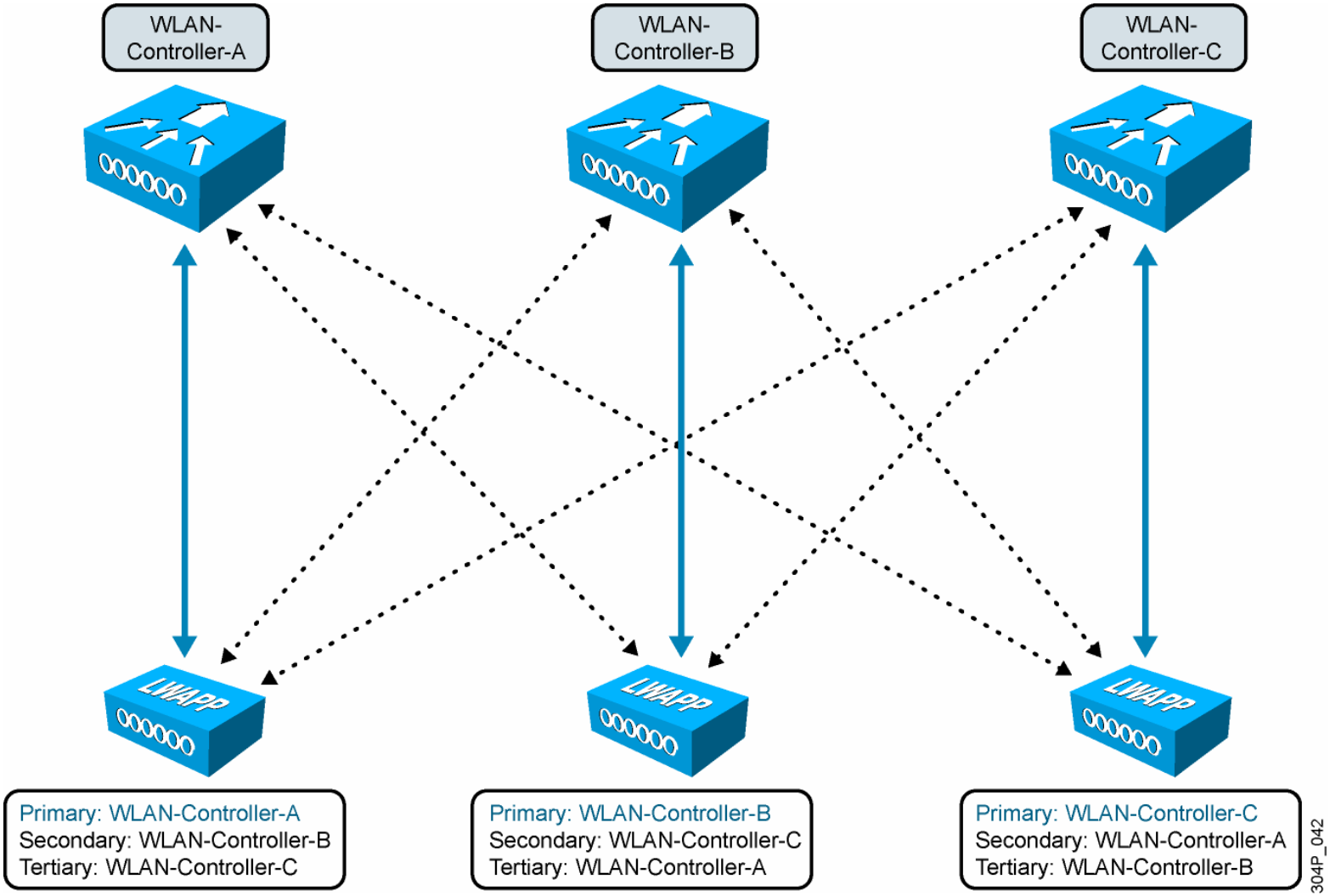
Access point selects its WLC with this sequence:

- [Deterministic] If an access point has been previously configured with a primary, secondary, or tertiary controller, the access point attempts to join these first (specified by controller sysName).
- [Initializing] The access point attempts to join a WLC configured as a master controller.
- [Dynamic] The access point attempts to join the WLC with the greatest availability for access point associations.

Deterministic Controller Redundancy

- Administrator statically assigns each access point a primary, secondary, or tertiary controller.
- Advantages include:
  - Predictability (easier operational management)
  - More network stability
  - More flexible and powerful redundancy design options
  - Faster failover times
  - “Fallback” option in the case of failover
- Disadvantages include:
  - More upfront planning and configuration
- Recommended leading practice is to use deterministic redundancy.

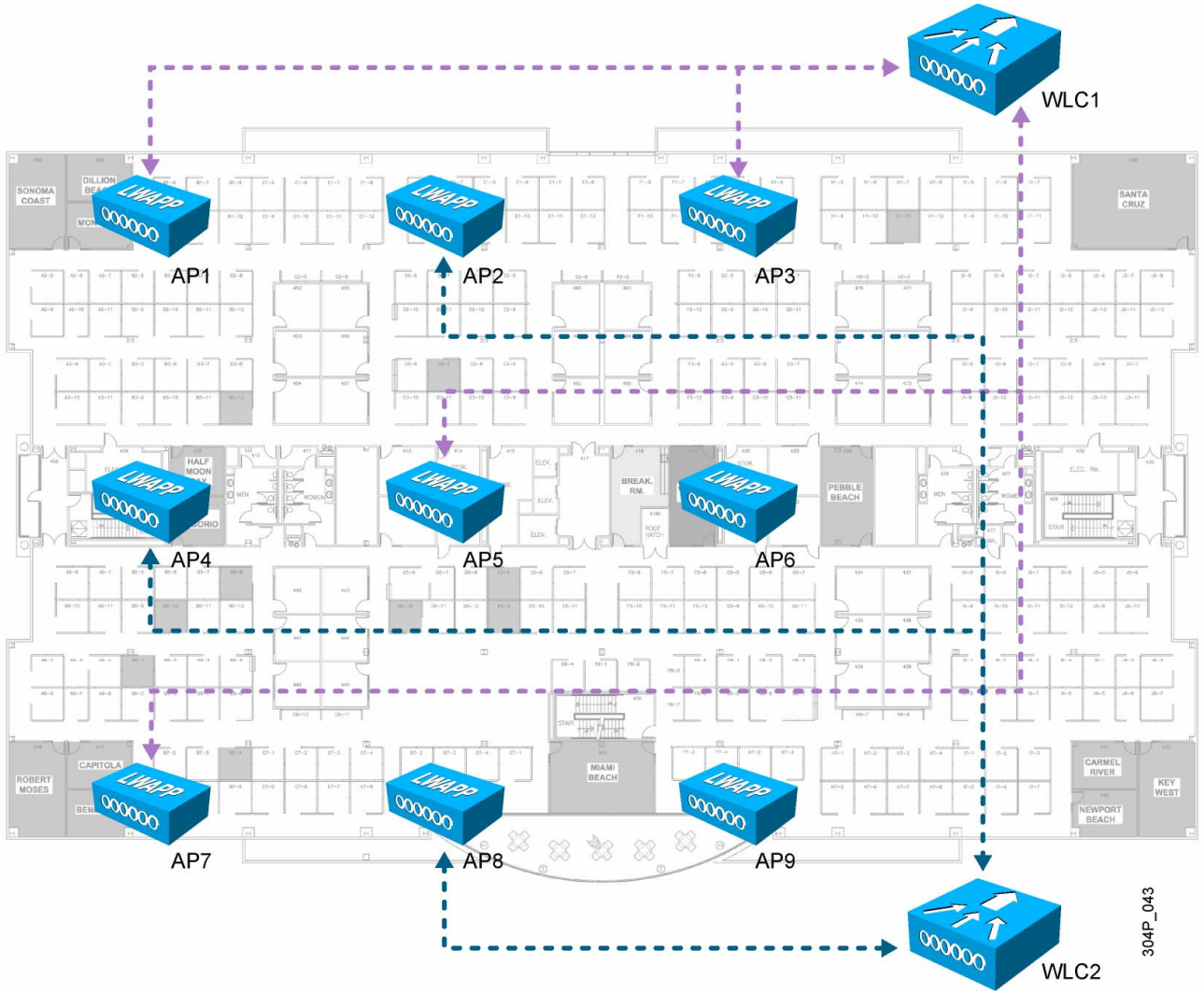
Example: Deterministic Controller Redundancy



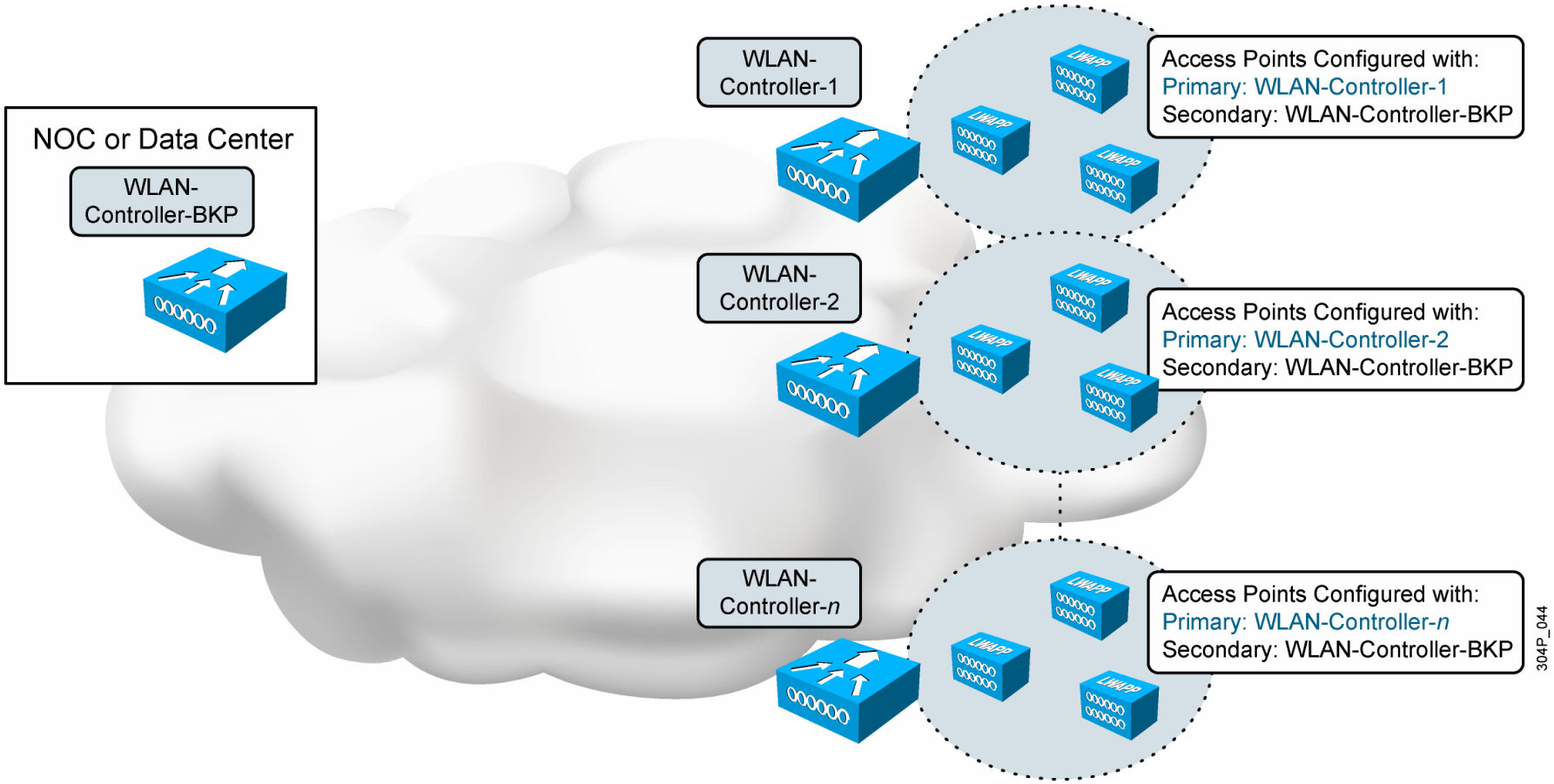
Dynamic Controller Redundancy

- Design relies on LWAPP to load-balance access points across controllers and populate access points with backup WLC information.
  - Design works better when controllers are “clustered” in a centralized design.
- Advantages include:
  - Easy to deploy and configure
  - Access points dynamically load-balance
- Disadvantages include:
  - More intercontroller roaming
  - Bigger operational challenges due to unpredictability
  - Longer failover times
  - No fallback option in the event of controller failure
- Recommended practice is not to use dynamic redundancy.

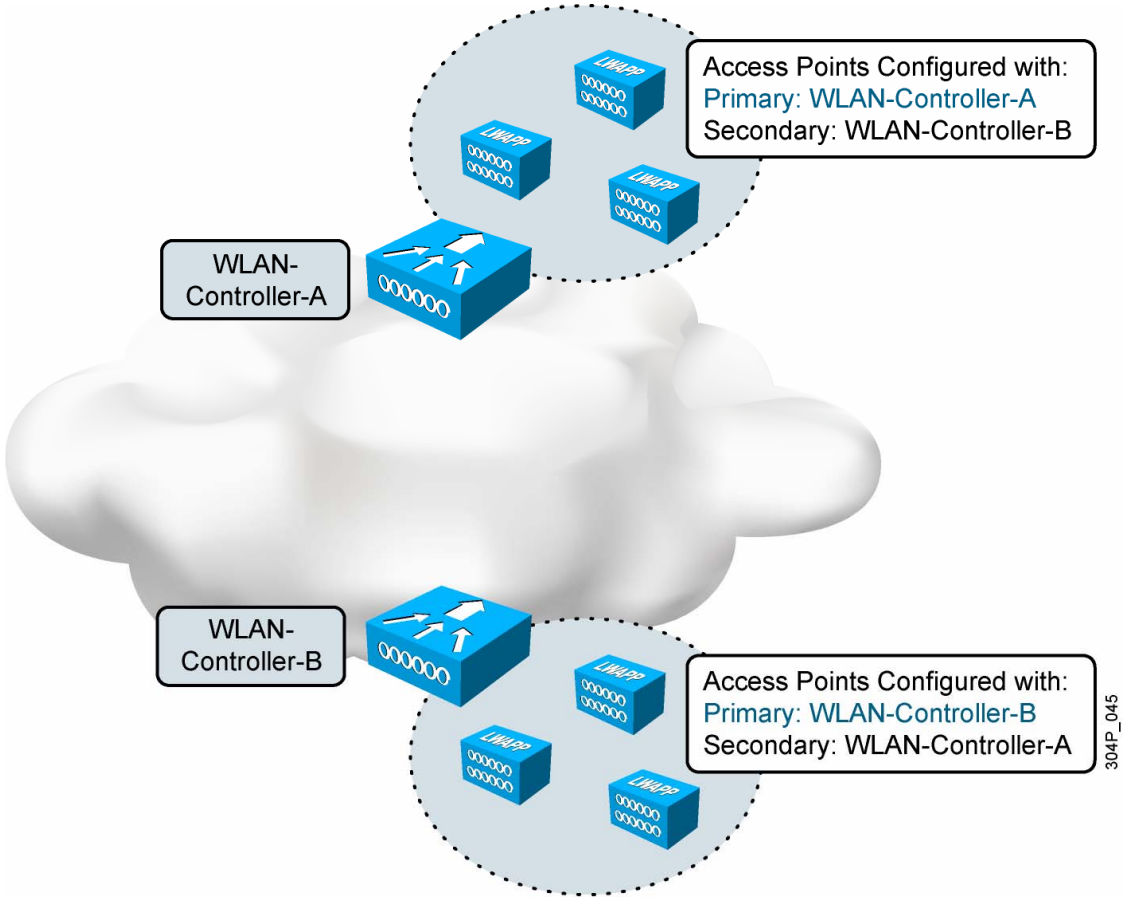
Example: Dynamic Redundancy



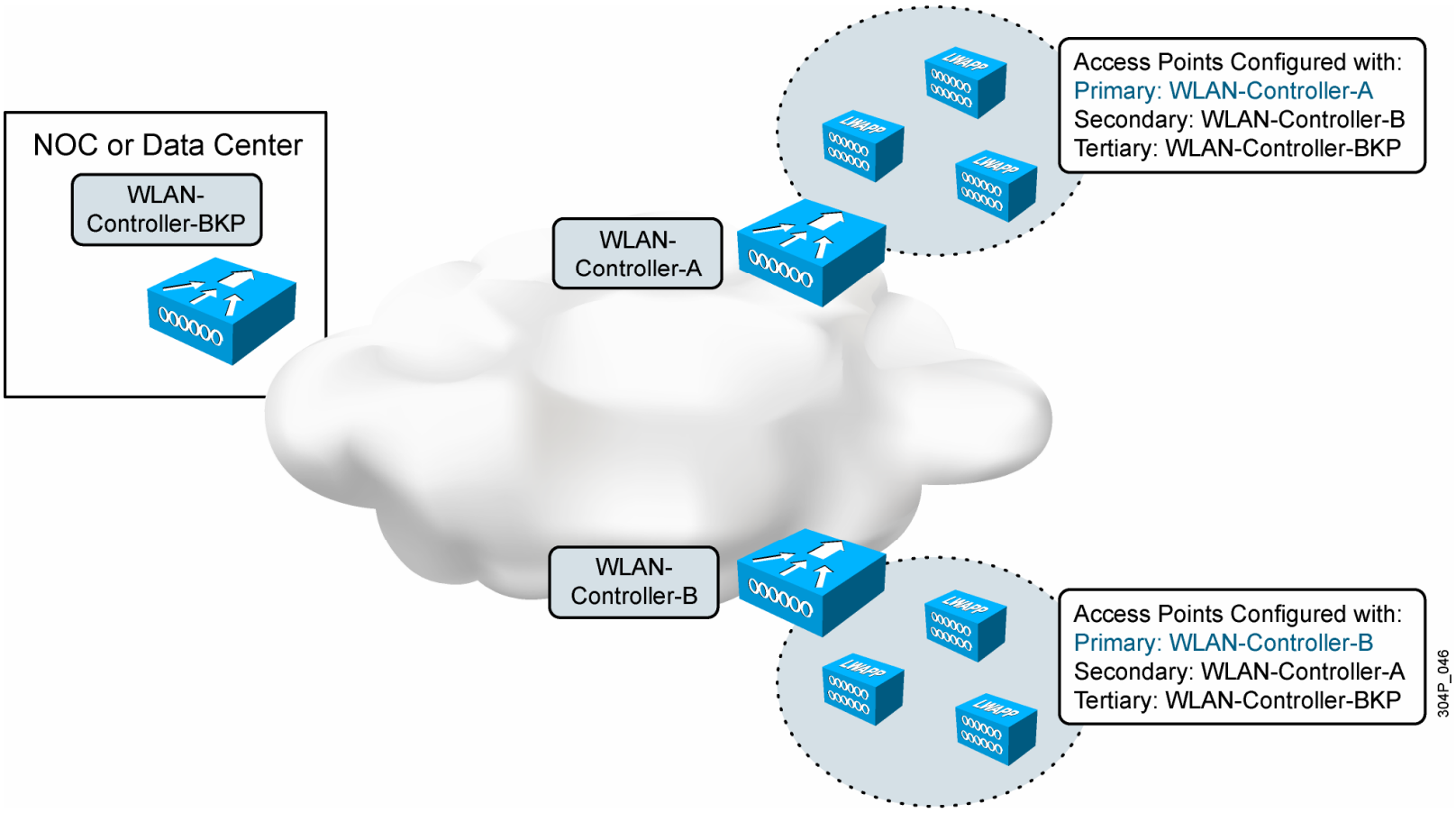
Deterministic Redundancy Designs: N + 1



Deterministic Redundancy Designs: N + N



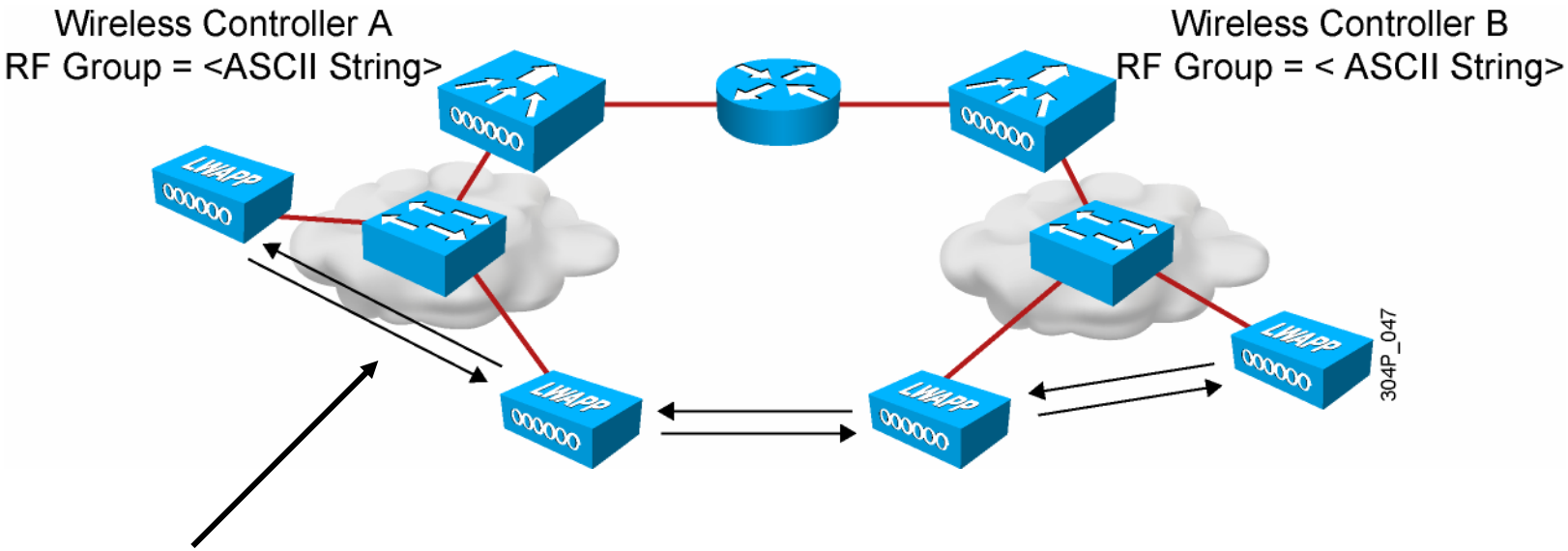
Deterministic Redundancy Designs: N + N + 1



Radio Resource Management

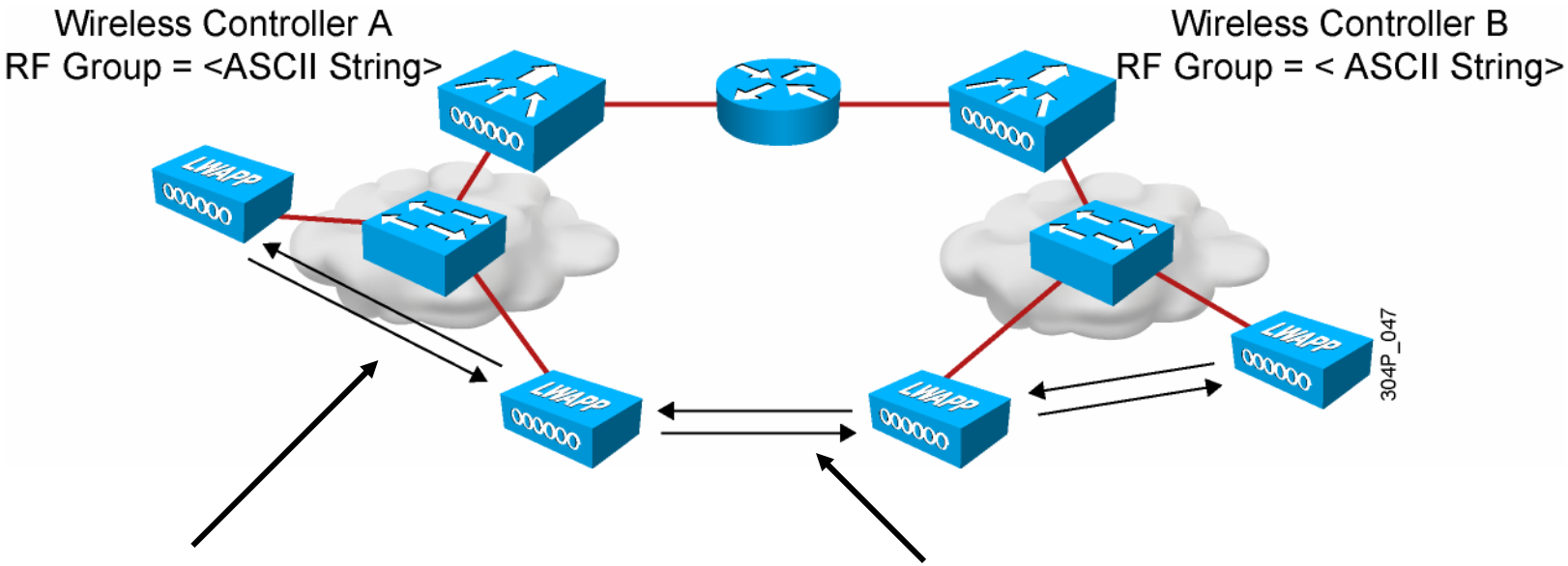
- Key RF challenges with 802.11:
  - Limited nonoverlapping channels
  - Physical characteristics of RF propagation
  - Contention for the medium
  - Transient nature of RF environments
- RRM addresses these challenges:
  - Continuous analysis of RF environment
  - Dynamic channel assignment
  - Interference detection and avoidance
  - Dynamic transmit power control
  - Coverage hole detection and correction
  - Client and network load balancing

RF Grouping



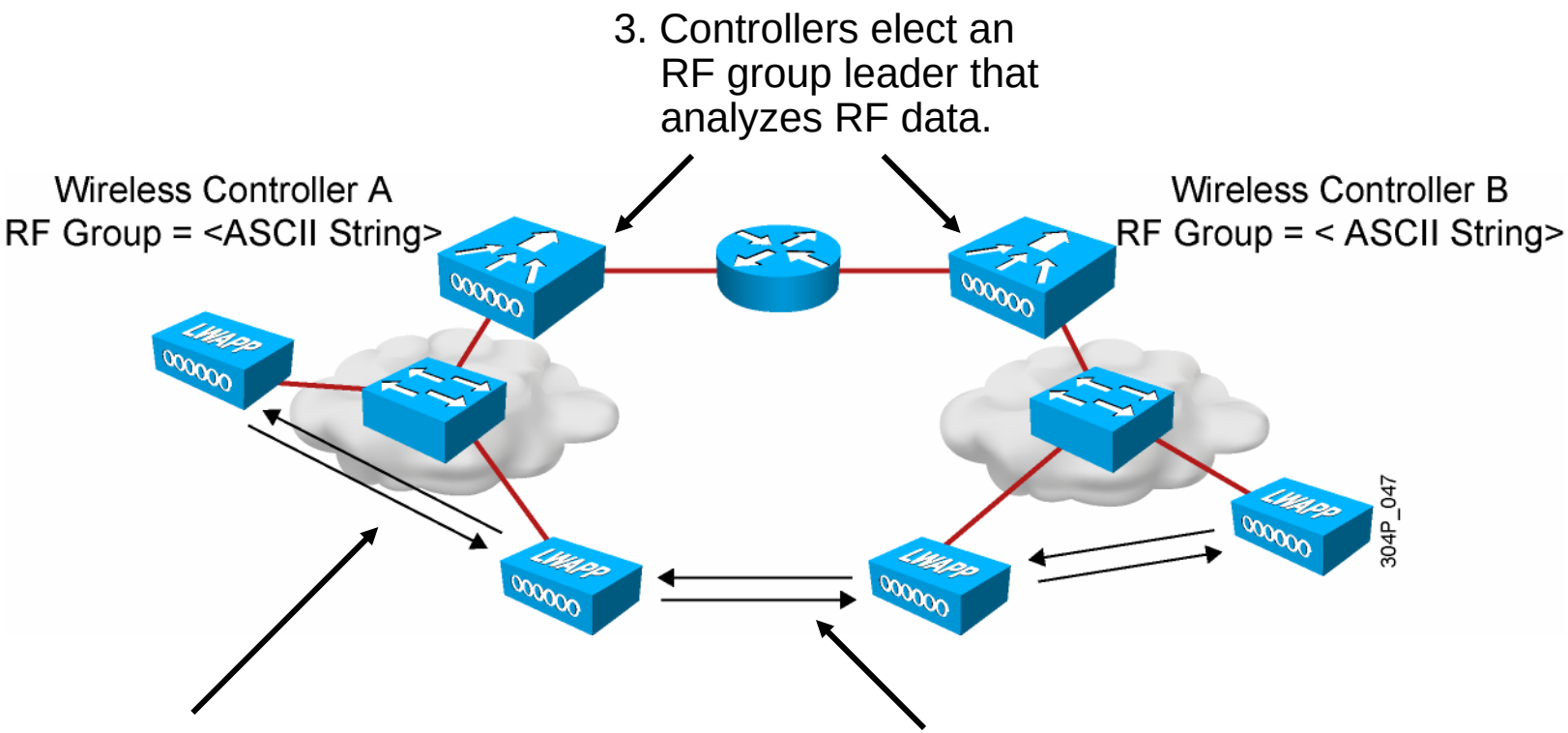
1. Access points send and receive neighbor messages.

RF Grouping



1. Access points send and receive neighbor messages.
2. If access points on different WLCs hear neighbor messages in the same RF group at -80 dBm or stronger, they pass information to their WLC.

RF Grouping



Access Point Self-Healing

- Access points receive neighbor messages from neighbor access points.
- Access points report a lost neighbor when they no longer receive neighbor messages at –65 dBm.
- RRM is used to increase power on access points near the lost access point.
- RRM can also adjust channel selection if needed.

Summary

- A lightweight access point uses an LWAPP discovery and join process to connect to a WLC.
- Lightweight access points operate by communicating with a WLC.
- The Cisco Unified Wireless Network provides a high quality transparent roaming experience for clients supporting both intracontroller and intercontroller roaming.
- It is recommended using that you use deterministic controller redundancy over dynamic controller redundancy.
- RRM using RF groups is a foundation of the Cisco Unified Wireless Network architecture.